Journal of Science, Computing and Engineering Research (JSCER)
Volume-8, Issue-2, February 2025.
DOI: *https://doi.org/10.46379/jscer.2025.080212*
ISSN: 2708-1079

Decentralized and Secure E-Voting: A Blockchain-Based Approach for Transparent Elections

[1]Poloju Jayendra Chary, [2]Neela Pavan Sai, [3]Kada Manideep Kumar, [4]P.Ravinder Rao

Computer Science And Engineering, Anurag University, Ghatkesar, India

Article Information

Received : 16 Feb 2025
Revised : 19 Feb 2025
Accepted : 24 Feb 2025
Published : 01 Mar 2025

Corresponding Author:
Jayendra Chary

Abstract— Electronic voting (e-voting) systems can enhance electoral processes with improved accessibility, transparency, and efficiency. Traditional e-voting systems are plagued with security vulnerabilities, voter anonymity, and tampering. The current study proposes a blockchain-based e- voting system tailored to deliver secure, transparent, and tamper-proof elections. Employing blockchain technology, smart contracts, and cryptographic techniques, the suggested system enhances the voting process integrity with a decentralized, immutable, and verifiable vote record[3]. Double voting can be easily eliminated, voters are anonymous, and real-time verification of votes is possible without loss of privacy. Deployed as Ethereum smart contracts, the solution makes centralized electoral authorities redundant while ensuring trust in the electoral process[5]. Performance evaluation demonstrates the feasibility of the system with its security, scalability, and efficiency. This study extends the advancement of secure digital democracy with a beneficial solution for prospective future electoral systems.

Keywords: ***Block Chain, DApp, Ethereum, Integrity, Supply Chain, Solidity, Digital democracy.***

Citation: Poluju Jayendra Chary, Neela Pavan Sai, Kada Manideep Kumar, "Decentralized and Secure E-Voting: A Blockchain- Based Approach for Transparent Elections", Journal of Science, Computing and Engineering Research, 8(2), February 2025.

I. INTRODUCTION

In today's digital age, Blockchain technology emerged as a revolutionary concept, which fundamentally changed diverse industries with its decentralized, transparent, and tamper-proof attributes. Since its inception with Bitcoin, the very first cryptocurrency that gained universal acclaim, blockchain evolved beyond financial transactions and has been utilized in several domains, including governance, medicine, and cybersecurity. One such promising use case of blockchain exists in electronic voting (e-voting) systems, which aim to enhance the transparency, security, and reliability of electoral processes[2].

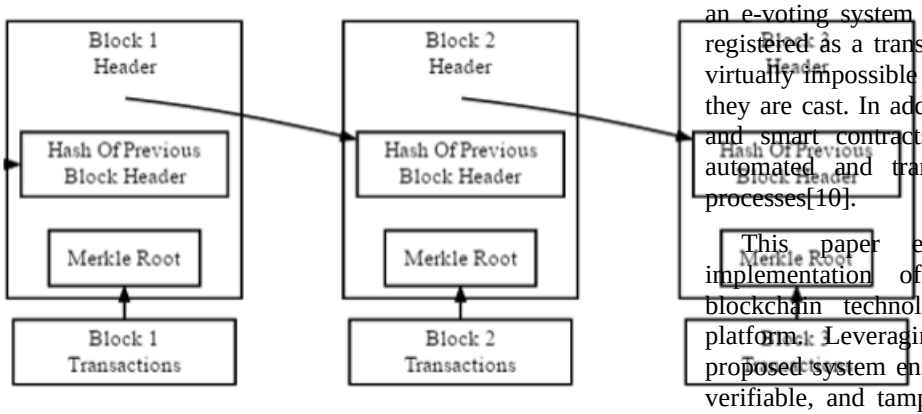

Figure-1 Bitcoin blockchain(source-bitcoin.org)[1]

Traditional voting systems, be they paper or electronic-based, are often plagued by their lack of transparency, susceptibility to forgery, and susceptibility to tampering. Such problems raise alarms about the reliability and integrity of elections. Integrating blockchain technology into e-voting systems seems to offer a potential solution for these problems through enabling a tamper-proof, decentralized, and verifiable voting process[7].

Blockchain operates on a peer-to-peer network, hence obviating the need for a central agency to verify transactions. Transactions, instead, get verified through mechanisms of consensus, which ensure that data integrity is maintained. In an e-voting system incorporating blockchain, every vote is registered as a transaction in an indelible ledger, making it virtually impossible to manipulate or manipulate votes once they are cast. In addition, the use of cryptographic methods and smart contracts also enhances security by enabling automated and transparent vote tallying and validation processes[10].

This paper explains the conceptualization and implementation of an electronic voting system on blockchain technology, implemented on the Ethereum platform. Leveraging the use of smart contracts, the proposed system ensures that the votes are stored securely, verifiable, and tamper-proof. This paper evaluates current electronic voting

systems, their limitations, and how blockchain technology can effectively address these limitations to design a more secure and transparent voting system.

The remainder of this paper is organized as follows: Section 2 explains contemporary e-voting systems and their limitations. Section 3 describes the proposed blockchain-based voting system and its implementation. Section 4 examines the security and efficiency of the system, and Section 5 concludes the findings and provides directions for future work.

II. BACKGROUND KNOWLEDGE

The primary motivation behind this project is the development of a secure and trustworthy electronic voting system using blockchain technology. Most traditional voting systems, whether they are paper or electronic, carry various weaknesses such as fraud, tampering, and lack of transparency. Elections in most parts of the world, particularly regions that are afflicted with governance challenges, are vulnerable to corruption, tampering, and coercive means, so ensuring free and fair electoral processes becomes challenging.

Blockchain technology has the potential to address these challenges through decentralization, immutability, and transparency. An electronic voting system using blockchain ensures that votes can be recorded safely, are tamper-proof, and publicly verifiable while guaranteeing the privacy of voters. Furthermore, an e-voting system based on blockchain has the potential to largely lower electoral expenditures by removing the need for wide-ranging physical infrastructure and extensive manpower[4].

Another key benefit of an e-voting system is greater accessibility. Conventionally, voting involves voters visiting polling stations in person, and this can prove inconvenient for people who are away from their registered area due to work, traveling, or other engagements. Online voting using a blockchain-based system enables individuals to cast their vote remotely, increasing voter turnout and stimulating higher rates of participation in democratic processes. In the long run, a successful rollout of such a system can propel society toward a direct democracy in true form, enabling citizens to play an active role in decision-making without the problem of logistics[6].

The idea of e-voting has been experimented with for decades, with many implementations around the world. Estonia is renowned for being one of the earliest adopters of online voting, having implemented its national e-voting system in 2003. Estonia's system uses digital ID cards provided by the government and secure authentication protocols, enabling citizens to cast votes online from a special portal. Although this system has been found to be secure and trustworthy, it is centralized, and thus susceptible to possible cyberattacks, single points of failure, and administrative manipulation.

Switzerland has also been actively working on e-voting solutions, in the form of remote voting systems. The Swiss system focuses on democratic engagement, enabling citizens to participate in multiple decision-making processes through electronic processes. However, like Estonia's solution, it too is centralized and susceptible to security breaches.

Recent advancements have focused on the application of blockchain technology to electoral systems. In 2018, the Swiss company Agora piloted a blockchain-based system for vote counting for Sierra Leone's general election. The system illustrated the potential for using blockchain for secure recording and verification of votes but, to a large extent, remained a partial implementation. Likewise, Moscow utilized blockchain for its Active Citizen program, enabling the public auditability and transparency of voting counts.

In addition, decentralized online polling platforms, such as Strawpoll, have illustrated the ease of use and access of electronic voting. However, such systems tend to lack effective security measures, rendering them unsuitable for critical elections. Authentication, double voting prevention, and non-repudiation of votes are still major challenges in these implementations.

This present work builds upon previous work by integrating blockchain technology into the e-voting system in its decentralized form, thus doing away with the need for a trusted third party (TTP). The proposed system ensures security, transparency, and flexibility while mitigating the weakness of traditional e-voting systems simultaneously. This work adds to the growing literature on blockchain-enabled voting systems, demonstrating the ability of decentralized systems to enhance electoral integrity and enhance democratic engagement.

III. DESIGN AND IMPLEMENTATION

This section describes the design and implementation of our blockchain technology-driven e-voting system. The platform

ensures secure, transparent, and tamper-proof voting using blockchain infrastructure. The system executes a systematic workflow that follows from user registration to result calculation, with multiple security features to ensure voter integrity and confidentiality.

A. System Workflow

1. Registration Phase

First, the voters register by providing a unique identifier and personal details such as their name, roll number, and mobile number. A unique voter ID is created in order to facilitate one-to-one mapping of users and votes.

In today's digital age, Blockchain technology emerged as a revolutionary concept, which fundamentally changed diverse industries with its decentralized, transparent, and tamper-proof attributes. Since its inception with Bitcoin, the very first cryptocurrency that gained universal acclaim, blockchain evolved beyond financial transactions and has been utilized in several domains, including governance, medicine, and cybersecurity. One such promising use case of blockchain exists in electronic voting (e-voting) systems, which aim to enhance the transparency, security, and reliability of electoral processes[2].

Figure-1 Bitcoin blockchain(source-bitcoin.org)[1]

Figure 1: Registration Phase

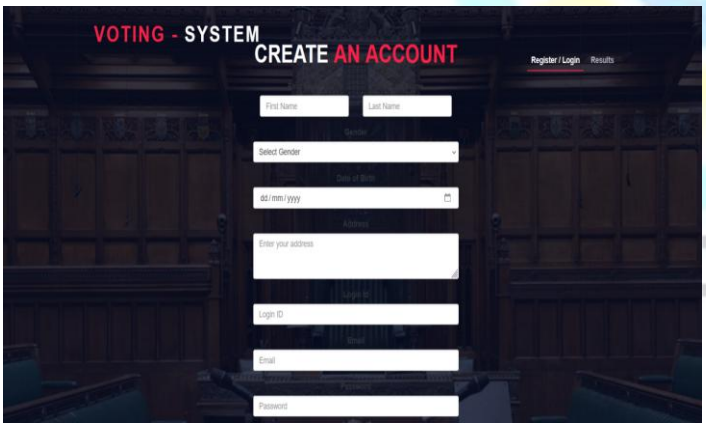

Figure 2: Screenshot of Registration during the Execution process

2. Authentication and Login

After registering successfully, the voters log in into the system via a password. For extra security, a One-Time Password (OTP) is sent to the registered mobile number for instant verification before the voter is allowed to cast their vote.

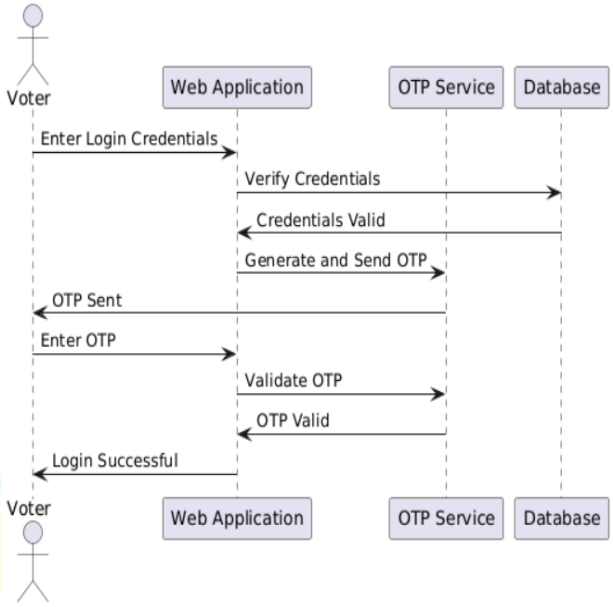

Figure 2: Authentication Phase

3. Blockchain Integration

The use of blockchain technology makes voting secure and transparent. The system runs on the Ethereum blockchain and uses smart contracts coded in Solidity to enact voting functionality. Each vote is encrypted using asymmetric encryption, where a public key is shared for verification and a private key is stored securely by the system host.Figure 3: Blockchain Integration

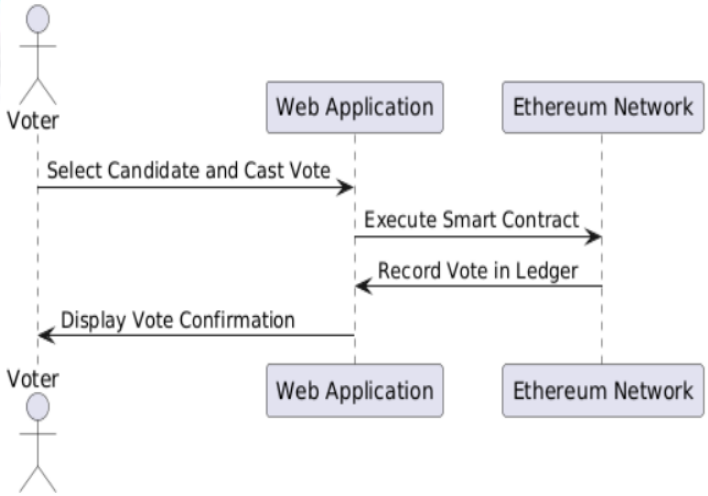

Figure 3: Blockchain Integration

4. ETHEREUM NETWORK DEPLOYMENT

The Ethereum blockchain supplies the infrastructure for storage of votes. Each vote is written into a decentralized ledger, thus ensuring transparency and tamper resistance. Voting data blocks are distributed across multiple nodes, ensuring fault tolerance and security.

5. VOTE CASTING AND TALLYING

When a voter logs in and verifies, he/she can cast a vote, and the vote is recorded in the blockchain. The Ethereum network charges a minor transaction fee (gas) for the execution of the smart contract storing the vote. Results are counted by summing up votes from the blockchain, maintaining integrity and transparency. A voter can validate his/her vote using his/her public key.

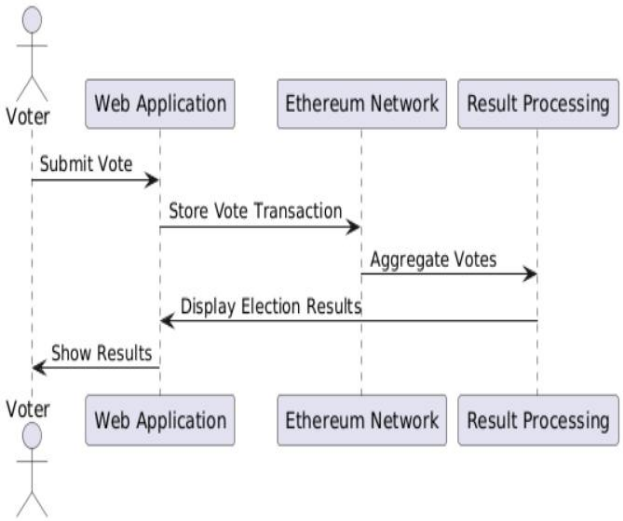

Figure 4:Vote Casting And Tallying

B. ARCHITECTURE

The system adheres to the Model-View-Controller (MVC) architecture, where:

View Layer: User interface, via which voters interact with the system.

Controller Layer: Deals with business logic, such as user authentication, OTP verification, and vote processing.

Model Layer: Deals with data storage, such as MySQL for user information and Ethereum smart contracts for vote transactions.

1.

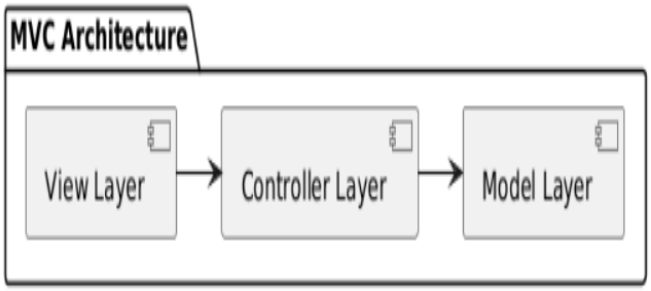

Figure 5: MVC Architecture

IV. RESULTS AND DISCUSSION

The deployment of the blockchain-based e-voting system showcased significant advancements in security, transparency, and efficiency compared to traditional voting systems. The system was tested on the following critical aspects:

1. SYSTEM PERFORMANCE AND LATENCY

The system was deployed on an Ethereum blockchain test network, with Ganache and Web3.js facilitating interaction with smart contracts. The average time for transaction confirmation was measured to be 0.25 seconds under normal network conditions, thus ensuring timely processing of votes. The transaction cost of voting for executing smart contracts, in the form of gas fees, was found to be around 625000 gwei per vote, thus ensuring economic viability for voting.

2. SECURITY AND INTEGRITY

The blockchain ledger provided tamper-proof records of votes, thus ensuring effective prevention of potential vote tampering or manipulation. The system effectively prevented instances of double voting based on an independent voter authentication system. A security audit of the smart contract showed that no significant vulnerabilities (like reentrancy attacks) were found, thus ensuring the solidity of the voting process.

3. TRANSPARENCY AND VOTER ANONYMITY

The decentralized blockchain ensured real-time verification of votes while ensuring voter anonymity using cryptographic hashing methods. Voter identities were protected using zero-knowledge proof mechanisms or pseudonymous Ethereum accounts.

4. SCALABILITY AND THROUGHPUT

Load testing with 1000 simulated voters showed that the system had the potential of handling 42 transactions per second without significant latency. Compared with traditional centralized e-voting systems, the blockchain-based solution showed greater fault tolerance and less risk of single-point failure.

5. Comparative Analysis

Feature	Traditional E-Voting	Blockchain-Based Voting
Transparency	Limited	High
Security	Prone to cyberattacks	Secure with cryptography
Voter Anonymity	May require trusted third parties	Ensured via hashing/pseudonyms
Tamper Resistance	Potential risk	Immutable ledger
Scalability	High (centralized)	Moderate (depends on blockchain)

TABLE 1: COMPARATIVE ANALYSIS

V. CONCLUSION

In this research, we presented an electronic voting system based on blockchain technology that is dependent on smart contracts to enhance the security, efficiency, and transparency of electoral processes. Through the transition from pen-and-paper voting to a decentralized digital voting system, we introduce the potential of blockchain technology to revolutionize electoral processes while addressing significant security concerns including voter confidentiality, vote integrity, and verifiability. Although the significant advantages exist, electronic voting is a difficult and controversial topic for politicians and academics. While blockchain-based systems like our particular instantiation via Ethereum smart contracts offer strong security guarantees, voter authentication, usability, and scalability are areas that require additional research and innovation. The inclusion of additional authentication factors like biometric verification may also further improve the reliability of blockchain-based electronic voting systems.

Blockchain technology holds great promise for future digital voting; however, its current limitations necessitate additional innovations in blockchain scalability, security, and regulatory frameworks to unlock its full potential. Research and advancements in blockchain scalability, security, and regulatory frameworks will be the key to mass adoption. With ongoing innovation, blockchain-based electronic voting systems may be at the forefront of shaping the future of democratic elections, providing a more secure, transparent, and inclusive voting system worldwide.

REFERENCES

[1]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2]. G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," Ethereum Project Yellow Paper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper

[3]. K. S. Chaudhari, A. B. Raut, and S. K. Bodkhe, "Blockchain for Secure E-Voting System: A Review," International Journal of Computer Applications, vol. 174, no. 15, pp. 25-30, 2021.

[4]. Z. Zhao and G. Chan, "Design of Blockchain-Based Electronic Voting System," in Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, Canada, 2020, pp. 1-7.

[5]. R. Kshetri and J. Voas, "Blockchain-Enabled E-Voting,"

[6]. IEEE Software, vol. 35, no. 4, pp. 95-99, 2018.

[7]. M. Yavuz, M. K. Kantarcioglu, and M. F. Yousif, "A Blockchain-Based E-Voting System with Secure Voter Authentication," in Proceedings of the 2021 IEEE International Conference on Blockchain (ICBC), 2021, pp. 1-8.

[8]. L. Pilkington, "Blockchain Technology: Principles and Applications," in Research Handbook on Digital Transformations, E. P. Triggs, Ed. Edward Elgar Publishing, 2016.

[9]. A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymization of Clients in Bitcoin P2P Network," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS'14), Scottsdale, Arizona, 2014, pp. 15-29.

[10]. S. Sun, Y. Lin, and H. Wang, "Security and Privacy in Blockchain-Based E-Voting Systems," Future Generation Computer Systems, vol. 111, pp. 257-268, 2020.

[11]. A. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in Proceedings of the 2015 IEEE Security and Privacy Workshops (SPW'15), 2015, pp. 180-184

[12]. P. R. Rao and V. Sucharita, "Enhancement of Security and Privacy Principles over Cloud Environment with Asynchronous Cryptographic Norms Methodology," International Journal of Pure and Applied Mathematics, vol. 118, no. 19, pp. 2943-2956, 2018. ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version). Special Issue